A Sturdy Security Framework for Security Challenges in Cognitive Radio Networks

Synopsis

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Electronics & Communication Engineering

Submitted by
Himanshu Sharma
11-Ph.D-028

Under the guidance of
Dr. Kuldip Pahwa
Asstt. Prof., ECE Department

Department of Electronics and Communication Engineering
M.M. Engineering College, Maharishi Markandeshwar University
Mullana (Ambala), 133207

ACKNOWLEDGEMENT

I would like to take this opportunity to express my gratitude to my supervisor Dr. Kuldip Pahwa, Asstt. Prof., ECE Deptt. for his persistent motivation, support and farsighted guidance. His broad knowledge and deep insights have been an important resource to me in completing this synopsis. I feel motivated and encouraged every time I attend his meeting. Without his encouragement and guidance this synopsis would not have materialized.

I would also like to show my greatest appreciation to Dr. H. P. Sinha, Prof. & Head, ECE Deptt. for all the support and motivation received so far. I would also like to thank the faculty members of ECE Department, MMEC for all the help and encouragement that I have received.

Also, special thanks to library staff for giving me support in collecting the material and books so far.

I am also deeply thankful to my parents, for their moral encouragement and financial support without which this synopsis would be difficult to complete.

Date:

Himanshu Sharma

Regn. No. 11-Ph.D-028
Mullana (Ambala)

ABSTRACT

Cognitive radio is widely expected to be the next Big Bang in wireless communications. Spectrum regulatory Committees in many countries have been taking steps to open the door to dynamic spectrum access using this technology and also laying down the rules for its implementation. A radio, therefore, that can sense and understand its local radio spectrum environment, to identify temporarily vacant spectrum and to use it, has the potential to provide wider bandwidth, increase spectrum efficiency and minimize the need for centralized spectrum management. This could be achieved by a radio that can make autonomous decisions about how it accesses spectrum intelligently. Cognitive radios have the potential to do this. In this Proposal, different security challenges in Cognitive radio networks have been studied and framework to combat the different security attacks on radio spectrum is proposed. So a robust security framework will be created to combat the effects of different attacks on cognitive radio networks.

LIST OF FIGURES

Figure 1.1	Cognitive Cycle	2
Figure 1.2	Technology Timeline	5
Figure 1.3	Physical Architecture of a Cognitive Radio	8
Figure 1.4	Cognitive Radio Network Architecture	10
Figure 1.5	Dynamic changes in all layers	13
Figure 2.1	Classification of various attack scenarios in CRN	20
Figure 3.1	Research Design	26

LIST OF TABLES

Table 3.1	Time Frame	27

LIST OF ABBREVIATIONS

CRN	Cognitive Radio Networks
CR	Cognitive Radio
FCC	Federal Communications Commission
SDR	Software Defined Radio
DARPA	Defence Advanced Research Projects Agency
IE	Incumbent Emulation
SSDF	Spectrum Sensing Data Falsification
PUE	Primary User Emulation

Table of Contents

Acknowledgement ..... **i**

Abstract ..... **ii**

List of Figures ..... **iii**

List of Tables ..... **iii**

List of Abbreviations ..... **iv**

CHAPTER 1: INTRODUCTION **1**

1.1 Introduction to Cognitive Radio 1

1.1.1 What is Cognitive Radio 1

1.1.2 Cognitive Cycle 2

1.2 History of Cognitive Radio 3

1.3 Cognitive Radio's Key Points 7

1.3.1 Cognitive Radio Architecture 7

1.3.2 Cognitive Radio Network Architecture 9

1.3.3 Cognitive Radio's key benefits 11

1.3.4 Characteristics of cognitive radios 13

1.3.5 Applications of Cognitive radios 14

1.4 Spectrum Sensing 15

1.5 Motivation 15

1.6 Aim & Objectives 16

1.7 Literature Review 17

CHAPTER 2: SECURITY ISSUES IN COGNITIVE RADIO NETWORKS **20**

2.1 Security issues related to CRNs 21

CHAPTER 3: RESEARCH METHODOLOGY & DESIGN APPROACH **24**

3.1 Overview of Problem 24

3.2 Problem Formulation & Research Methodology 24

3.3 Research Design 25

3.4 Time Frame 27

REFERENCES **28**

Chapter-1

Introduction

This chapter presents information about Cognitive radio system, their history, overview, applications, and their benefits. All the aspects related to cognitive radio networks are covered in this chapter. Finally this chapter ends with research objective and aim of the research with key literature review.

1.1 Introduction to Cognitive Radio

The concept of cognitive radio was first proposed by Joseph Mitola III in a seminar at KTH (the Royal Institute of Technology in Stockholm) in 1998 and published in an article by Mitola and Gerald Q. Maguire, Jr. in 1999. [23]

1.1.1 What is a cognitive Radio?

There are likely to be a variety of different views of what exactly would be a cognitive radio may be. Accordingly a definition of a cognitive radio may be of use in a number of instances.

"A cognitive radio may be defined as a radio that is aware of its environment and the internal state and with knowledge of these elements and any stored pre-defined objectives can make and implement decisions about its behavior" [6].

"In general the cognitive radio may be expected to look at parameters such as channel occupancy, free channels, the type of data to be transmitted and the modulation types that may be used. It must also look at the regulatory requirements. In some instances knowledge of geography and this may alter what it may be allowed to do" [25].

According to Federal Communications Commission (FCC): "Cognitive radio: A radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify the system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets [8].

Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit-

power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind:

• Highly reliable communications whenever and wherever needed;

• Efficient utilization of the radio spectrum.

Six key words stand out in this definition: awareness, intelligence, learning, adaptivity, reliability, and efficiency. Implementation of this far-reaching combination of capabilities is indeed feasible today, thanks to the spectacular advances in digital signal processing, networking, machine learning, computer software, and computer hardware.

1.1.2 Cognitive cycle

The cognitive capability of a cognitive radio enables real time interaction with its environment to determine appropriate communication parameters and adapt to the dynamic radio environment.

The tasks required for adaptive operation in open spectrum are shown in Figure 1.1 [4], which is referred to as the cognitive cycle. The three main steps of the cognitive cycle, shown in Figure 1.1, are as follows:

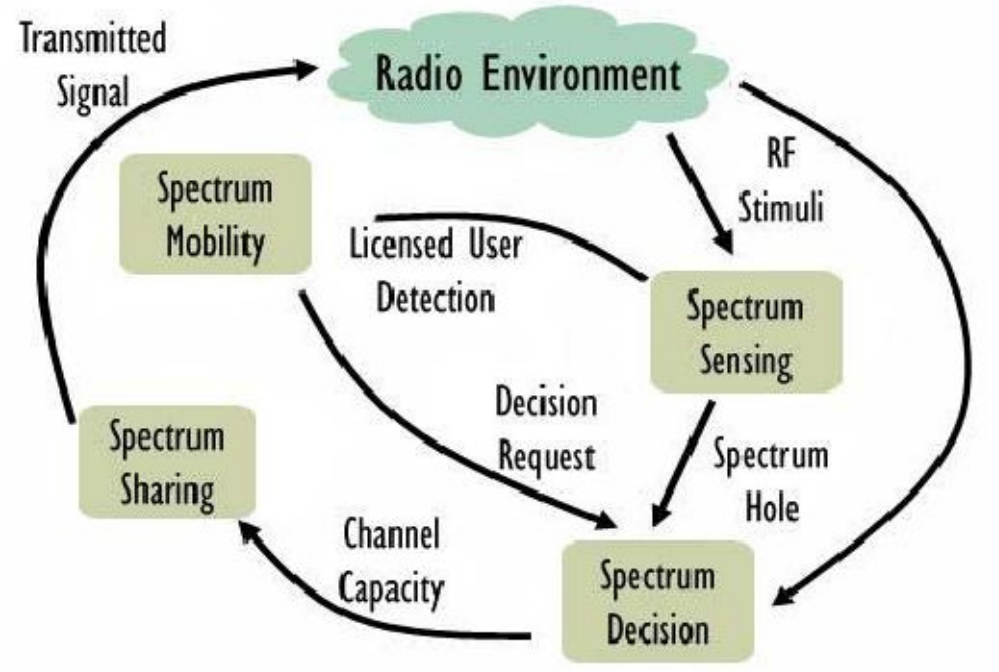


Figure 1.1 Cognitive Cycle

• **Spectrum sensing:** Detecting unused spectrum and sharing the spectrum without harmful interference with other users.

• **Spectrum management**: Capturing the best available spectrum to meet user communication requirements.

• **Spectrum mobility**: Maintaining seamless communication requirements during the transition to better spectrum.

• **Spectrum sharing**: Providing the fair spectrum scheduling method among coexisting cognitive users.

1.2 History of Cognitive Radio

The sophistication possible in a software-defined radio (SDR) has now reached the level where each radio can conceivably perform beneficial tasks that help the user, help the network, and help minimize spectral congestion. Radios are already demonstrating one or more of these capabilities in limited ways. A simple example is the adaptive digital European cordless telephone (DECT) wireless phone, which finds and uses a frequency within its allowed plan with the least noise and interference on that channel and time slot. Of these capabilities, conservation of spectrum is already a national priority in international regulatory planning.

Major applications that raise an SDR's capabilities and make it a cognitive radio:

1. Spectrum management and optimizations.

2. Interface with a wide variety of networks and optimization of network resources.

3. Interface with a human and providing electromagnetic resources to aid the human in his or her activities.

There are many technologies have come together to drive cognitive radio techniques, with a few of the major contributions that have led up to today's cognitive radio developments have been mentioned. The development of digital signal processing (DSP) techniques arose due to the efforts of such leaders as Alan Oppenheim, Lawrence Rabiner, Ronald Schaefer, Ben Gold, Thomas Parks, James McClellen, James Flanagan, fred harris, and JamesKaiser. These pioneers recognized the potential for digital filtering and DSP, and prepared the seminal textbooks,

innovative papers, and breakthrough signal processing techniques to teach an entire industry how to convert analog signal processes to digital processes.

They guided the industry in implementing new processes that were entirely impractical in analog signal processing.

Cleve Moler, Jack Little, John Markel, Augustine Gray, and others began to develop software tools that would eventually converge with the DSP industry to enable efficient representation of the DSP techniques, and would provide rapid and efficient modeling of these complex algorithms.

Meanwhile, the semiconductor industry, continuing to follow Moore's law, evolved to the point where the computational performance required implementing digital signal processes used in radio modulation and demodulation were not only practical, but resulted in improved radio communication performance, reliability, flexibility, and increased value to the customer.

During this same period, researchers all over the globe explored various techniques to achieve machine learning and related methods for improved machine behavior. Among these was analog threshold logic, which leads to fuzzy logic and neural networks, a field founded by Frank Rosenblatt.

In networking, DARPA (Defence Advanced Research Projects Agency) and industrial developers at Xerox, BBN Technologies, IBM, ATT, and Cisco each developed computer-networking techniques, which evolved into the standard Ethernet and Internet we all benefit from today. The Internet Engineering Task Force (IETF) and many wireless-networking researchers continue to evolve networking technologies with a specific focus on making radio networking as ubiquitous as our wired Internet. These researchers are exploring wireless networks that range from access directly via a radio access point to more advanced techniques in which intermediate radio nodes serve as repeaters to forward data packets toward their eventual destination in an ad hoc network topology.

All of these threads come together at the cognitive radio era (see Figure 1.2). Cognitive radios have applications that sit on top of an SDR, which in turn is implemented largely from digital signal processors and general-purpose processors (GPPs) built in silicon. In many cases, the spectral efficiency and other intelligent support to the user arises by sophisticated networking of

many radios to achieve the end behavior, which provides added capability and other benefits to the user.

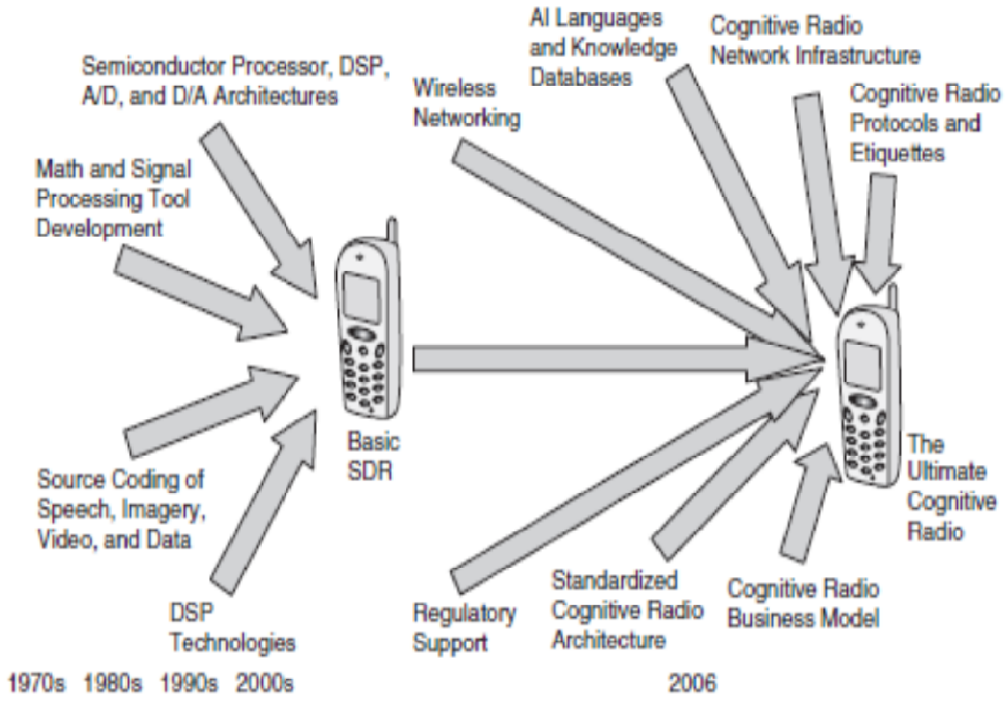


Figure 1.2 Technology timeline. Synergy among many technologies converge to enable the SDR. In turn, the SDR becomes the platform of choice for the cognitive radio.

In order to alleviate the spectrum scarcity, cognitive radio (CR) has been introduced to facilitate the spectrum sharing to increase the spectrum efficiency so that the larger density of wireless users can be accommodated without creating a new RF spectrum band.

Chronology of opportunistic spectrum

• 1999–2000 (United States): Localized set of measurements conducted by the DARPA indicated that spectrum use was not very high.

• 2002 (United States): DARPA initiates the XG (Next Generation) project to investigate the potential for the military to share spectrum spatially and temporally with multiple devices.

• 2002 (United States): The FCC Spectrum Policy Task Force (SPTF) concludes that spectrum access is a more significant problem than spectrum scarcity. The SPTF recommends that new

rules be developed to allow more intensive access to the spectrum, including opportunistic spectrum.

• 2003 (European Union): IST includes DSA technologies as part of the sixth Framework Program of R&D.

• 2003 (United States): The NSF initiates research projects in spectrum measurements and DSA.

• 2004 (United States): The FCC issues a Notice of Proposed Rulemaking on Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies.

Although the term Cognitive Radio has been defined originally as an extension to software radios ([23] introduced originally in [24]), which is able to provide reason about external factors. Recently the term Cognitive Radio is mostly used in a narrower sense. FCC suggests that any radio having the adaptive spectrum awareness should be referred to as "Cognitive Radio".

A cognitive radio / spectrum pooling architecture have been developed at the University of Karlsruhe. Weiss and Jondral in 2004 have defined a centralized spectrum pooling architecture based on OFDM. They envision an 802.11 like access-point based scenario for the cognitive radio system consisting of a cognitive radio base-station and cognitive radio mobile users and do not assume any changes to licensed user systems. Using OFDM has the advantage to be able to feed certain sub-carriers with zeros resulting in no emission of radio power on these carriers (occupied by licensed users). The use of OFDM also enables the analysis of the spectral activity of licensed users at no extra cost, as an FFT is required anyway.

DARPA followed a much more general approach and tries to define an architectural framework based on a "vision" paper within the Next Generation (XG) program to implement policy based intelligent radios. DARPA's XG aims to address the problem of having radios with regulable kernels, which can be controlled via policy rules. This allows radios to transcend regulatory borders with simple policy changes. XG radios are capable of sensing the environment to determine unused spectrum (opportunity awareness), use policy constraints to allocate these channels (opportunity allocation) among a group of radios that together form an XG-domain and to determine mechanisms for using those channels (opportunity use). As with any multi-user

network, centralized and distributed variants of the three functions (awareness, allocation and use) are possible.

Regulatory domains are realizing the need for new technologies in order to efficiently using available spectral resources as well. Recent studies by the Federal Communications Commission's (FCC) Spectrum Policy Task Force (SPTF) have reported vast temporal and geographic variations in the usage of allocated spectrum with utilization ranging from 15% to 85% [8]. In order to utilize these 'white spaces', the FCC has issued a Notice of Proposed Rule Making [9] advancing Cognitive Radio (CR) technology.

1.3 Cognitive Radio's key points

1.3.1 The Cognitive Radio Architecture

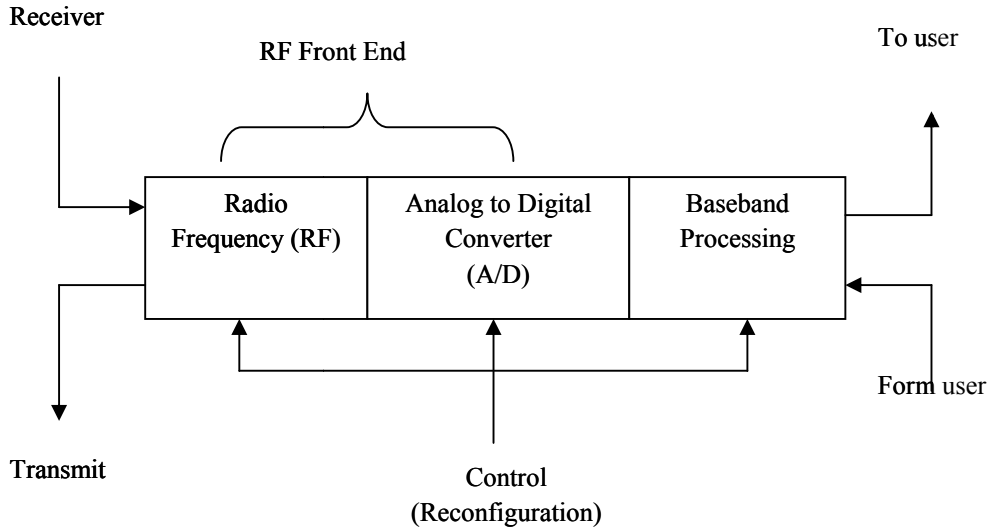
CR is defined as a radio that can "change its transmitter parameters based on interaction with its environment".

From this definition, two main characteristics of cognitive radio can be defined

• Cognitive capability: Through real-time interaction with the radio environment, the portions of the spectrum that is unused at a specific time or location can be identified. CR enables the usage of temporally unused spectrum, referred to as spectrum hole or white space. Consequently, the best spectrum can be selected, shared with other users, and exploited without interference with the licensed user.

• Re-configurability: A CR can be programmed to transmit and receive on a variety of frequencies, and use different access technologies supported by its hardware design. Through this capability, the best spectrum band and the most appropriate operating parameters can be selected and reconfigured.

In order to provide these capabilities, CR requires novel radio frequency (RF) transceiver architecture. The main components of a CR transceiver are the radio front-end and the baseband processing unit that was originally proposed for software-defined radio (SDR), as shown in figure below.



(a)

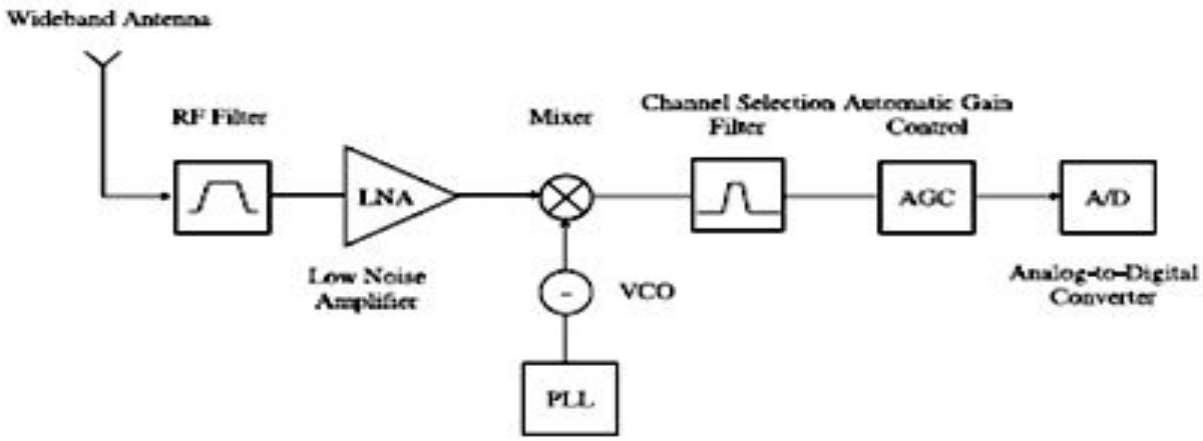


Figure 1.3:– Physical architecture of the cognitive radio: (a) Cognitive radio transceiver and (b) wideband RF/analog front-end architecture.

The components of a cognitive radio RF front-end are as follows:

• RF filter: The RF filter selects the desired band by band pass filtering the received RF signal.

• Low noise amplifier (LNA): The LNA amplifies the desired signal while simultaneously minimizing noise component.

• Mixer: In the mixer, the received signal is mixed with locally generated RF frequency and converted to the baseband or the intermediate frequency (IF).

• Voltage-controlled oscillator (VCO): The VCO generates a signal at a specific frequency for a given voltage to mix with the incoming signal. This procedure converts the incoming signal to baseband or an intermediate frequency.

• Phase locked loop (PLL): The PLL ensures that a signal is locked on a specific frequency and can also be used to generate precise frequencies with fine resolution.

• Channel selection filter: The channel selection filter is used to select the desired channel and to reject the adjacent channels. There are two types of channel selection filters. The direct conversion receiver uses a low-pass filter for the channel selection. On the other hand, the super-heterodyne receiver adopts a band pass filter.

• Automatic gain control (AGC): The AGC maintains the gain or output power level of an amplifier constant over a wide range of input signal levels.

1.3.2 The Cognitive Radio Network Architecture

Existing wireless network architectures employ heterogeneity in terms of both spectrum policies and communication technologies. Moreover, some portion of the radio spectrum is licensed for different technologies and some bands remain unlicensed (called Industrial Scientific Medical (ISM) band). A clear description of Cognitive Radio Network architecture is essential for the development of communication protocols.

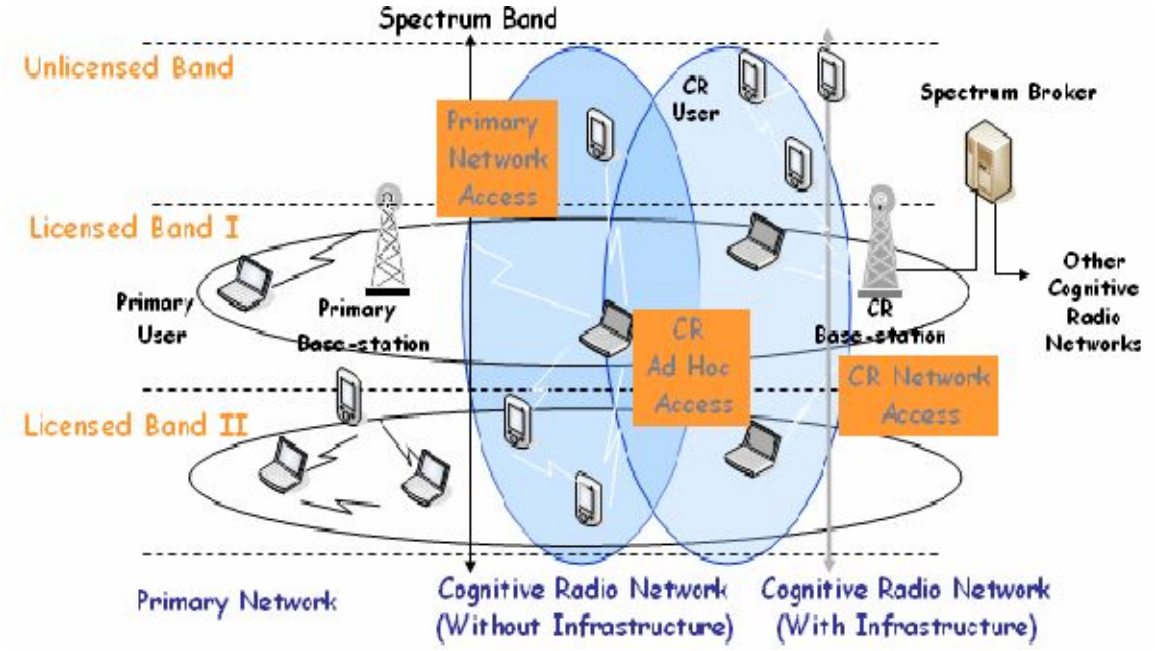


Figure 1.4 Cognitive Radio Network Architecture [27]

The components of the Cognitive Radio network architecture, as shown in Figure 1.4, can be classified in two groups such as the primary network and the CR network. The basic elements of the primary and the CR network are defined as follows:

• **Primary network**

A network with rights for a specific radio spectrum band is called primary network. Examples include the common cellular network, WiMAX, CDMA and TV broadcast networks. The components of the primary network are as follows.

Primary user

A user of primary network which has a license to operate in a certain spectrum band. Primary user has access to the network via base-station. All of its services and operations are controlled by base-station. Hence, it should not be affected by any unlicensed user or user of any other network. Therefore, primary users do not need any change for coexistence with Cognitive Radio base-stations and Cognitive Radio users.

Primary base-station

A fixed infrastructure network component for a specific technology with licensed band is called a Primary base - station. Examples are base-station transceiver system (BTS) in a cellular system

and BTS in WiMAX etc. Primary base-station does not have the capability for coexisting with Cognitive Radio Network, hence, the primary base-station require some modifications such as the need to have both licensed and Cognitive Radio protocols present for the primary network access of CR users.

• **Cognitive Radio network**

A network where the spectrum access is allowed only in opportunistic manner and does not have license to operate in a desired band is called Cognitive Radio Network. It can be deployed both as an infrastructure network and an ad hoc network as shown in Figure 1.4. The components of a CR network are as follows:

Cognitive Radio user

Cognitive Radio user or secondary user has no spectrum license for its operation so some additional functionality is required to share the licensed spectrum band.

Cognitive Radio base-station

Cognitive radio base-station or secondary base-station is a fixed infrastructure component that provides a single hop connection to Cognitive Radio users without any license of radio spectrum. Cognitive Radio users can access the other networks with the help of this connection.

Spectrum broker

Spectrum broker is a central network entity that provides the sharing of spectrum resources among different CR networks. Hence, spectrum broker can be connected to each network like star topology in Networks and can act as centralized server having all information about spectrum resources to enable coexistence of multiple CR networks.

1.3.3 Cognitive Radio's key benefits

Cognitive Radio offers optimal diversity (in frequency, power, modulation, coding, space, time, polarization and so on) which leads to:

• **Spectrum Efficiency**- This will allow future demand for spectrum to be met and is the basic purpose of implementing CR.

• **Higher bandwidth services-** Demand of MBMS (Multimedia Broadcast Multicast service) is constantly on the rise which will be facilitated by the implementation of CR.

• **Graceful Degradation of Services -** When conditions are not ideal, a graceful degradation of service is provided, as opposed to the less desirable complete and sudden loss of service. This feature of CR is very important in providing services to the users especially when they are mobile and the base stations in contact are constantly changing.

• **Improved Quality of Service (QoS)** (latency, data rate, cost etc) - Suitability, availability and reliability of wireless services will improve from the user's perspective.

• **Commercial Exploitation**- CR promotes spectrum liberalization (makes it much easier to trade spectrum between users). Indeed, a business case may exist for becoming a spectrum broker, whereby a third party manages the trade between supplier and demander and receives a commission.

• **Benefits to the Service Provider**- More customers in the market and/or increased information transfer rates to existing customers. More players can come on the market.

• **Future-proofed product**- A CR is able to change to services, protocols, modulation, spectrum etc. without the need for a user and/or manufacturer to upgrade to a new device.

• **Common hardware platform**- Manufacturers will gain from economies of scale because they no longer need to build numerous hardware variants, instead using a single common platform to run a wide range of software. This also assists in the rapid service deployment.

• **Flexible regulation**-By using a form of policy database, regulation could be changed relatively quickly as and when required, easing the burden on regulators.

• **Emergency service communications**- Joint operations during major incidents would benefit greatly as police, fire, ambulance and coastguard could be linked together in one radio with each radio user sensing the spectrum being used by the other parties and reconfiguring itself.

• **Benefits to the Licensee**- CR can pave the way for spectrum trading, where licensees would be allowed to lease a portion of their spectrum rights to third parties on a temporal, spatial or other appropriate basis to recoup some of the expense of its 24hr-a-day license and even make money.

1.3.4 Characteristics of Cognitive Radios

Cognitive radio dynamically selects the frequency of operation and also dynamically adjusts its transmitter parameters. The main characteristics of cognitive radios are Cognitive Capabilities and Re-configurability.

• **Cognitive Capability**

Cognitive capability refers to the ability of radio to sniff or sense information from its environment and perform real time interaction with it. The cognitive capability can be explained with the help of three characteristics; Spectrum Sensing, Spectrum Analysis and Spectrum Decision. The spectrum sensing performs the task of monitoring and detection of spectrum holes. The spectrum analysis will estimate the characteristic of detected spectrum hole. In the spectrum decision, the appropriate spectrum is selected by determining the parameters like data rate, transmission mode etc.

• **Re-configurability**

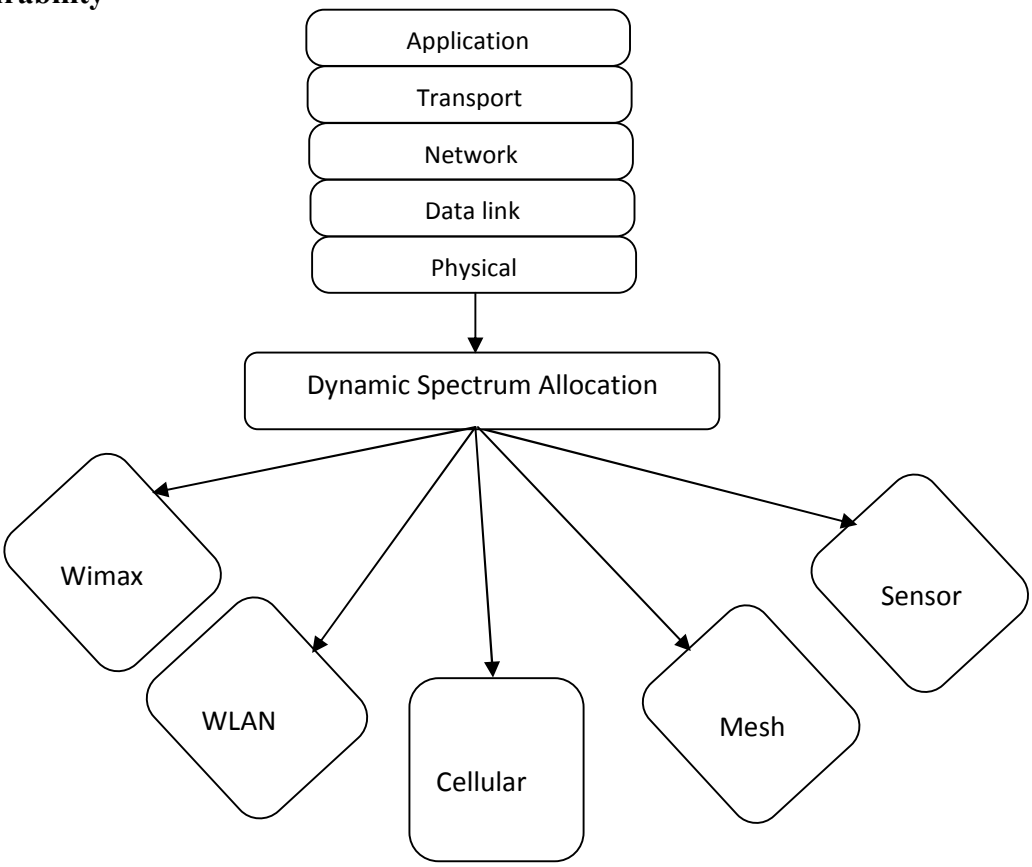


Figure 1.5 Dynamic changes in all Layers

Re-configurability refers to the ability of radio that allows the cognitive radio to adjust its parameters like links, operating frequency, modulation and transmission power at run time without any modifications in the hardware components. In other words Re-configurability of CR is SDR.

Doing so, there is a change in all the layers of communication as shown in Figure 1.5. Different technologies depending on their spectrum availability with the same hardware can be used.

1.3.5 Applications of Cognitive Radios [28]

Cognitive Radio Networks can be applied to the following cases:

• **Leased network**

The primary network may provide a leased network by allowing cognitive radio user to access its licensed spectrum in an opportunistic manner without harming the communication of the primary user.

• **Cognitive mesh network**

For providing broadband connectivity wireless mesh networks are emerging as a cost-effective technology [17]. However mesh networks require higher capacity to meet the requirements of the applications that demand higher throughput. Since the cognitive radio technology enables the access to larger amounts of spectrum, therefore cognitive radio networks will be a good choice to meet the requirements of mesh networks.

• **Emergency network**

Cognitive Radio Networks can be implemented for Public safety and emergency networks. In the case of natural disasters, when primary networks are temporarily disabled their spectrum band can be used by CR users. CR networks can communicate with available spectrum band in ad hoc mode without the need for an infrastructure and by maintaining communication priority and response time.

• **Military network**

CR networks are used in the military radio environment. CR networks can enable the military radios to choose arbitrary intermediate frequency (IF) bandwidth, modulation schemes, and coding schemes, adapting to the variable radio environment of the battlefield.

1.4 Spectrum Sensing

Spectrum sensing is the art of performing measurements on a part of the spectrum and forming a decision related to spectrum usage based upon the measured data. In recent years, the service providers are faced with a situation where they require a larger amount of spectrum to satisfy the increasing quality of service (QoS) requirements of the users. This has raised the interest in unlicensed spectrum access, and spectrum sensing is seen as an important enabler for this. In a scenario in which there exist a licensed user (primary user), any unlicensed (secondary) user needs to ensure that the primary user is protected, i.e., that no secondary user is harmfully interfering any primary user operation. Spectrum sensing can be used to detect the presence (or absence) of a primary user. Recently, FCC regulations have paved way for utilizing spectrum obtained from unused TV channels, the so-called TV white spaces. In these regulations, spectrum sensing plays a major role.

When spectrum sensing is performed using a single sensor, that sensor may be in a deep fade, e.g., it may be shadowed, relative to a transmitter one wishes to detect. This is known as the *hidden node problem*. Because of this possibility a secondary unit basing its decisions on single sensor sensing may not engage in a secondary transmission unless it is highly confident in its detection of a spectrum opportunity, i.e., it must be able to detect a transmitter even as it experiences deep fading. To this end, the sensing node must use conservative detection thresholds and/or highly sensitive receivers, which cause high *false alarm* probability (the probability of reaching a "detect" decision when there was nothing there) and high cost devices, respectively. An approach that does not possess the above disadvantages, but requires some coordination, is cooperative sensing in which multiple sensors are utilized.

1.5 MOTIVATION

In the past ten years, a dramatic growth in wireless communication due to the popularity of smart phones and other mobile devices is witnessed. As a result, the demand for commercial spectrum has been skyrocketing. There is an increase in demand for unlicensed bandwidth, due to the

continuing growth of as Wi-Fi, and emergence of application domains, such as sensor networks for safety applications, home automation, smart grid control, medical wearable and embedded wireless devices, and entertainment systems. Meeting this huge demand for bandwidth is a challenge since most easily usable spectrum bands have been allocated. Many studies have however shown that more than 90% of the allocated spectrum is unused or underutilized. This suggests that meeting future demands for wireless bandwidth will not only require new communication and networking technologies that use the spectrum more efficiently (i.e. increase bits/second/Hz), but also new techniques for increasing spectrum utilization. Cognitive radios are widely viewed as the disruptive technology that can radically improve both spectrum efficiency and utilization. Cognitive radios are fully programmable wireless devices that can sense their environment and dynamically adapt their transmission waveform, channel access method, spectrum use, and networking protocols as needed for good network and application performance. One of the applications of cognitive radio is more efficient, flexible, and aggressive dynamic spectrum access

1.6 AIM & OBJECTIVES

AIM: The major aim of this research is to evaluate the impact of different attacks on efficiency of cognitive radio network and to develop novel spectrum sensing approach by using two stage spectrum sensing or other approach to monitor the health of cognitive radio.

OBJECTIVES:

Major Steps involved in this research are listed below:

- To Study, design & develop a Cognitive Radio network.
- To evaluate the impact on efficiency of Cognitive radio network by applying different attacks (e.g. PUE, Sensor Jamming, Incumbent Emulation and Spectrum Sensing Data Falsification).
- To use Frequency hopping technique and error detection codes to combat the effect of Incumbent Emulation.
- To develop novel spectrum sensing approach using two stage spectrum sensing or other relevant technique.

- Checking the Robustness of designed system.

1.6 Literature Review:

Alexander W. Min et.al. [1] introduces a new framework called SOLID for accurate/ fault-tolerant tracking of small scale mobile primary users ion CRN. By jointly performing localization and shadow fading estimation, SOLID significantly improves the accuracy of mobile primary user tracking and masks the effect of manipulated sensing reports by accurately detecting and filtering them out.

A.D Domenico et.al. [2] presents two stage spectrum sensing for cognitive radio networks. They also provides the different MAC layer strategies for CRN. Functionalities of MAC layer in CRN were identified.

A. Attar et.al. [3] contributed much in security challenges in CRNs. They provide a complete survey of different security challenges in Cognitive radio networks along with solutions and future research directions. Future research directions include a robust cognitive communications. They provide a new idea of robustness of Cognitive radio networks. An overview was also given about incentive based security mechanisms and reliable spectrum sensing schemes. Introduction to CRN specific security threats were given which includes Infrastructure based CRN attacks and Infrastructure-less CRN attacks.

O. Leon et.al. [7] presented the potential attacks against CRN and their countermeasures. Networks were classified into centralized, partially distributed and fully distributed and the attacks whether attacker is a part of CRN or not (insider or outsider).

T. Yucek et.al. [8] presented the spectrum opportunity and spectrum sensing concepts are re-evaluated by considering different dimensions of the spectrum space. The new interpretation of spectrum space creates new opportunities and challenges for spectrum sensing while solving some of the traditional problems. Various aspects of the spectrum sensing task are explained in detail. Several sensing methods are studied and collaborative sensing is considered as a solutionto some common problems in spectrum sensing. Pro-active approaches are given and sensing methods employed in current wireless systems are discussed. Estimation of spectrum

usage in multiple dimensions including time, frequency, space, angle, and code; identifying opportunities in these dimensions; and developing algorithms for prediction into the future using past information can be considered as some of the open research areas.

T. Qin et.al. [10] proposed a novel trustaware hybrid spectrum sensing scheme which can detect misbehaving secondary users and filter out their reported spectrum sensing results from the decision making process. The robustness and efficiency of the proposed scheme are verified through extensive computer simulations. A CRN can be deployed in several configurations such as centralized, distributed, ad-hoc or mesh networks. In this paper, only the centralized infrastructure based network is investigated.

T.C Clancy [13] presented new class of attacks specific to cognitive radio networks. Wireless devices that can learn from their environment can also be taught things by malicious elements of their environment. They focus primarily on PHY-layer issues, describing several classes of attacks and giving specific examples for dynamic spectrum access and adaptive radio scenarios. These attacks demonstrate the capabilities of an attacker who can manipulate the spectral environment when a radio is learning. The most powerful of which is a self-propagating AI virus that could interactively teach radios to become malicious. Then they describe some approaches for mitigating the effectiveness of these attacks by instilling some level of "common sense" into radio systems, and requiring learned beliefs to expire and be relearned.

Ian F. Akyildiz et.al. [17] presented many research issues need to be resolved for wireless mesh networks that are scalability, self-organization and self configuration, security, network integration.

A.Ghasemi et.al. [18] presented the effect of user collaboration on the performance of sensing-based secondary access in fading channels has been investigated. In particular, under independent fading or shadowing, a low-overhead collaboration scheme with a very simple detector as its building block: 1) improves the spectrum utilization significantly, 2) enables the individual users to employ less sensitive detectors, thereby allowing a wider range of devices to access the primary bands, 3) increases the robustness toward noise uncertainty, 4) reduces the

time and bandwidth resources required for satisfactory sensing which translates into higher agility and efficiency of the secondary access.

Chapter-2

Security Issues in Cognitive Radio Network

This chapter presents an overview of several security threats related with Cognitive Radio environment. Here mainly three types of CRN specific issues including Sensor jamming, Incumbent Emulation and Spectrum Sensing Data Falsification (SSDF) are presented.

Cognitive Radio (CR) is a new technology that promises to solve the spectrum shortage problem by allowing secondary users to coexist with primary users without causing interference to their communication. Cognitive radio technology is Opportunistic by nature, means in any spectrum if there is spectrum hole (i.e. part of spectrum is not utilized by primary user) then cognitive radio can transmit on that particular band. Due to its opportunistic behavior there exist several security threats to CRNs. Some of which are discussed below:

There are two main types of security issues related with Cognitive Radio Networks [2]:

1. Traditional (general) security concerns, which are similar to other wireless communication systems.
2. CRN specific security threats.

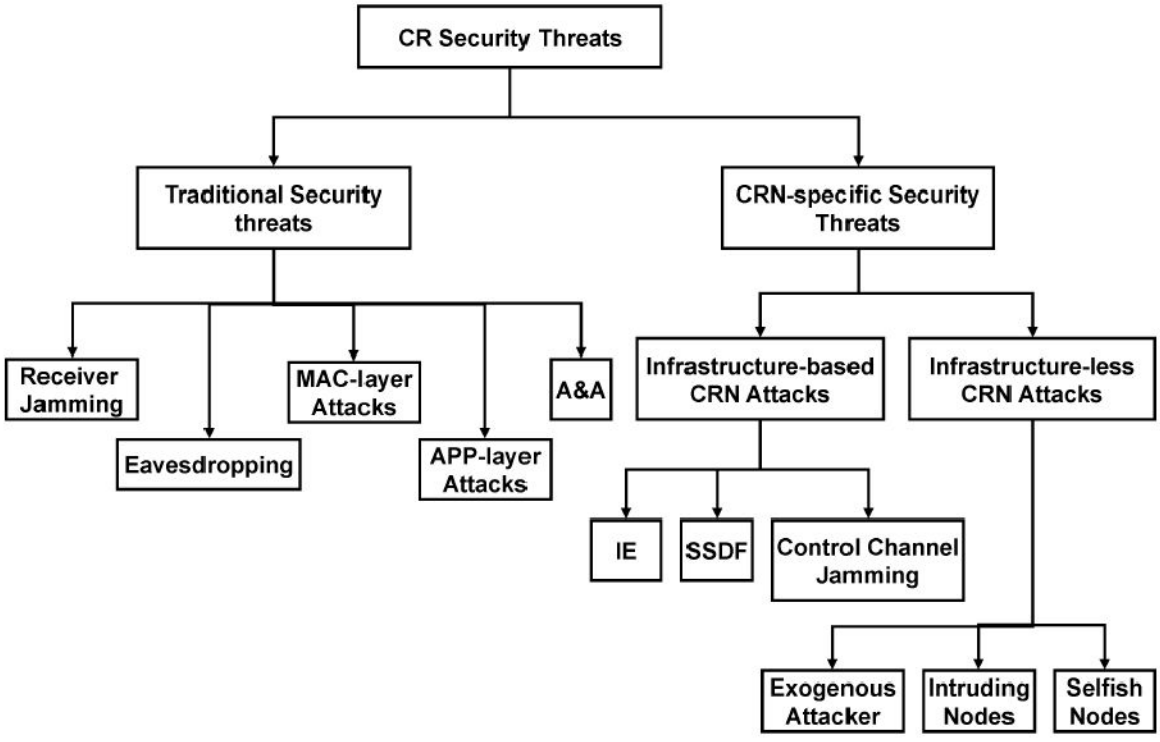


Figure 2.1 Classification of various attack scenarios in CRN [2]

The CRN architecture can be infrastructure based, for e.g. the IEEE 802.22 standard, or infrastructure-less, such as ad hoc CRN.

2.1 Security Issues related to CRNs:

Infrastructure based CRN Specific Security Attacks:

Centralized CRNs such as based on IEEE 802.22 standard architecture follows cellular architecture and controlled by a centralized Base Station. All network related tasks are performed by base station itself. Cognitive Radio networks are more likely to be affected by external interference. Hence it is most important to discuss all types of security threats related with base station.

Dynamic Spectrum Attacks: The first type of attack is *Primary User Emulation* (PUE) attack, and can be effective in dynamic spectrum access (DSA) environments. In such environments, a primary user owns a license to a particular frequency band, and can use it whenever they wish. When they are idle, secondary devices can opportunistically use the available spectrum. Such secondary devices need spectrum sensing algorithms to detect when the primary user is active. Hence it is easier for an attacker to interference in such system. There are two types of attacks which fall in this category:

1. Jamming:
2. Incumbent Emulation

Jamming Attack: An external adversary node is not part of the CRN and thus not part of the CRN's spectrum sensing decision making. However, such external attackers can affect the successful operation of a CRN through jamming attacks. In sensor-jamming attacks an attacker floods the sensed channel with white/colored noise. The jamming signal will increase the received SNR at the local energy detection sensing nodes. The secondary then assumes that increased SNR is due to presence of primary, which in turn implies false determination of channel state.

Incumbent Emulation: Feature detection can provide a more reliable primary detection strategy, which makes it more difficult for a sensor jammer to mount a jamming attack on the

CRN. Instead, the adversary node(s) can deter the CRN from accessing a given primary channel by transmitting a signal closely matching the primary's waveform. This type of attack is generally known as IE/Incumbent Emulation and is having severe effects on CRNs.

Intruding Attacks: CRNs are vulnerable to attacks from intruding adversary nodes which can penetrate into the network posing as legitimate nodes. The infiltrated malicious node can influence the overall spectrum sensing decision of CRN mainly via reporting misleading local sensing data. This class of CRN-specific security issue is known as the spectrum sensing data falsification (SSDF).An intruding attacker can initiate an SSDF-style attack by providing the central decision making entity within an infrastructure-based CRN with misleading sensing data. Given the centralized process of authorization and authentication (A&A) of nodes in an infrastructure-based CRN, however, it is more challenging for an adversary node to infiltrate the CRN network**.**

Infrastructure less CRN Specific Attacks:

CRN-specific security threats from infrastructure-less CR settings have been investigated. The main source of security threats in a distributed CRN setting is manipulation of a spectrum sensing process by the adversaries. The sophistication of attack strategy depends on factors such as the spectrum sensing technique exploited by the CRN and possibility/simplicity of intrusion to the CRN, among other factors. To provide an insightful description of infrastructure-less CRN attacks, the attackers are differentiated as exogenous attackers, intruding nodes and greedy CRs.

A. Exogenous Attackers

An external adversary node is not part of the CRN and thus not part of the CRN's spectrum sensing decision making. However, such exogenous attackers can affect the successful operation of an ad hoc CRN through jamming attacks. The target of jamming attack can be the DSS (Distributed Spectrum Sensing) process or else it can affect the common control channel of the CRN. Furthermore, if the CRN utilizes a feature-detection spectrum sensing strategy, the exogenous attacker can follow incumbent emulation (IE) attacks.

Jamming: Using energy detection for spectrum sensing in ad hoc CRNs opens the network to CRN-specific sensor-jamming attacks where an attacker floods the sensed channel with white/colored noise. The jamming signal will increase the received SNR at the local energy detection sensing nodes. Therefore, an exogenous attacker can also disrupt the operation of a CRN by transmitting jamming signals over such common control channel. This type of an attack is known as control channel jamming

Incumbent Emulation (IE): Feature detection can provide a more reliable primary detection strategy, which makes it more difficult for a sensor jammer to mount a DoS (Denial of Service) attack on the CRN. Instead, the adversary node(s) can deter the ad hoc CRN from accessing a given primary channel by transmitting a signal closely mimicking the primary's waveform. This type of attack is generally known as IE.

B. Intruding Attackers

Ad hoc CRNs are vulnerable to attacks from intruding adversary nodes which can penetrate into the network posing as legitimate nodes. The infiltrated malicious node can influence the overall spectrum sensing decision of CRN mainly via reporting misleading local sensing data. This class of CRN-specific security issue is known as the spectrum sensing data falsification (SSDF). The simplest type of SSDF attacks is performed by always reporting a channel busy or idle. More complex attackers selectively provide false spectrum sensing reports so as to keep their attack strategy more difficult to identify.

C. Greedy CRs:

In ad hoc CRNs, a degree of competition in utilizing the available spectrum resources exists. This competition might motivate some greedy CRs, which unlike intruding nodes are authenticated and authorized members of the CRN, to misbehave in order to increase their chances of reserving the medium. In its natural extent, greedy behavior of CR nodes is known to reduce the total network capacity compared to a cooperative networking strategy. As an example, if the CRN MAC scheme follows ALOHA-style handshaking with random backoff mechanism, a greedy CR can manipulate the backoff window so as to increase its probability of access to the spectrum.

Chapter-3

Research Methodology & Design Approach

This chapter presents an overview of problem of security in CRNs. It highlights the research methodology employed to design the new algorithm, with the purpose to meet the requirements of development of robust CRN. Finally, the chapter summarises the research design and approach, which describes the major steps involved in research to be undertaken in this project.

3.1 Overview of Problem:

As it clear from discussion in previous chapter that Cognitive Radio Networks are vulnerable to several attacks and different security issues. Hence for proper operation of any CRN there should be proper signal processing algorithm to combat the effect of the attackers and make the communication more reliable and secure. As cognitive radio is new emerging technology literatures don't have much idea about which security algorithm is to be adapted.

3.2 Problem Formulation & Research Methodology

By way of Cognitive Radio technologies established, the concerns of operational robustness and security considerations gain increasing prominence. Like any supplementary wireless communication technology, a comprehensive scrutiny of steadfastness and security challenges in Cognitive Radio Networks is a crucial stair toward realization of real-world solutions. The major objective of this research is to propose new schemes in order to make solution for Security Challenges in Cognitive Radio Networks, to manage the spectrum efficiently and to maximize the network performance. As an initial phase, the objective is to manage the spectrum and to control the behavior of intruders.

The security contemplations in Cognitive Radio Network scenery are still in their infancy phase and require a more thorough exploration by the research community. A number of threats and intimidations specifically pertain to cognitive communications, most conspicuously to secure the spectrum sensing process against exogenous and insider malicious nodes. It is further crucial to more closely examine other attacks including incumbent emulation (IE) attacks, primary user emulation attacks and sensor jamming. The far reaching effect of isolated attacks against

Cognitive Radio Networks, due to the learning-based collaboration Cognitive Radio nodes with their radio frequency environment, is another key concern to be more vigorously investigated. One of aim is to use technology which overwhelmed such attack mechanism in the network. Frequency hopping, error detection code, shadow fading filter etc. are certain available technologies which is best suited in such attack mechanism for adaptive channel sensing.

One of the important concerns is these sensing mechanisms are primarily used to identify if there is an incumbent transmitting, and if there is a need to avoid interfering with it. Therefore two stages fast and fine sensing in module is to be added. The MAC layer will perform two different types of sensing in either in-band or out-of-band measurements: fast sensing and fine sensing. Fast sensing will consist in sensing at speeds of under some milliseconds per channel. This sensing is performed by the device and the BS and the BS's will gather all the information and will decide if there is something new to be done. The fine sensing takes more time and it is used based on the outcome of the previous fast sensing mechanism.

There is need of certain technologies which overcome the effect of attack in the network, there are few points which inspires us in making the solution as mentioned.

A common trait in all these attacks is the need for more interference-resilient communications schemes, for instance, to decode the received signals in very low SNR regimes or to detect the primary signal buried in the jammer’s signal.

It is of utmost importance to develop adaptive strategies based on CRN learning capability to align the link and the system level requirements and to improve the overall network performance.

3.3 Research Design

The major steps involved in this research proposal are summarized in figure given below and are explained briefly.

The first step in research proposal is to review the security mechanism related to Cognitive radio networks and the different types of attacks. After that needs and research objectives are defined. Now the main research work starts with designing of cognitive radio network and applying different types of attacks to the network. After that health of cognitive radio network is

monitored. Next step is to apply different techniques to combat the effect of different security attacks and to develop a spectrum sensing approach by using two stage spectrum sensing. Finally robustness of the designed system is checked and findings are to be made.

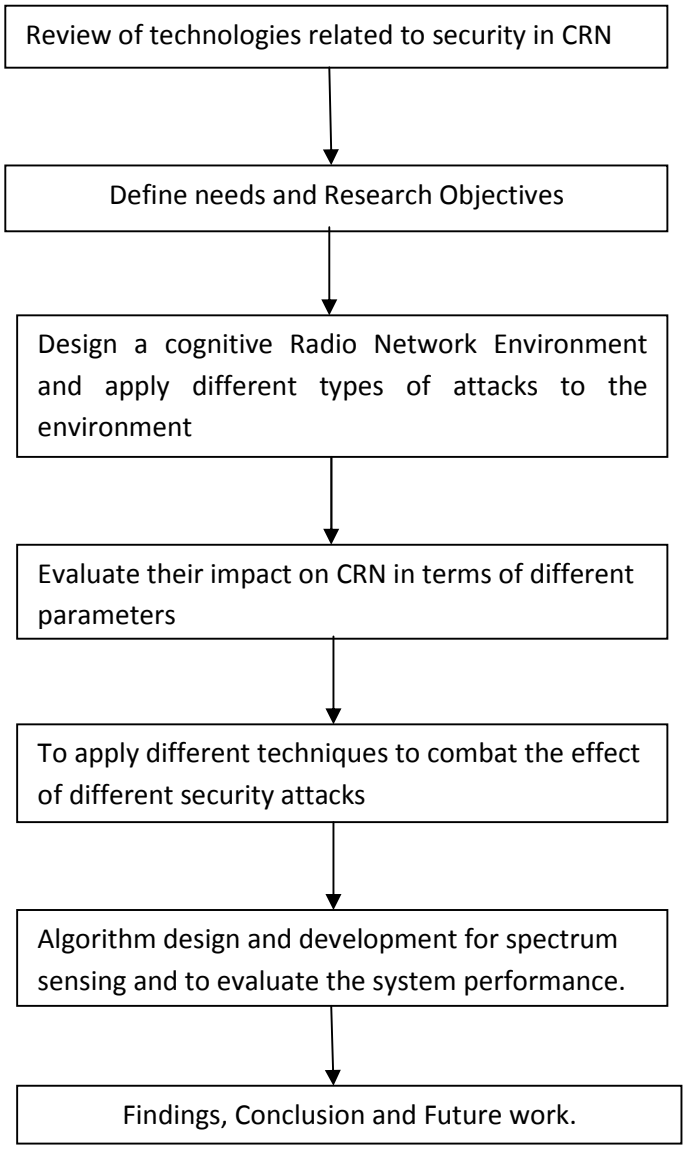

Review of technologies related to security in CRN
Define needs and Research Objectives
Design a cognitive Radio Network Environment and apply different types of attacks to the environment
Evaluate their impact on CRN in terms of different parameters
To apply different techniques to combat the effect of different security attacks
Algorithm design and development for spectrum sensing and to evaluate the system performance.
Findings, Conclusion and Future work.

Figure 3.1 Research Design

3.4 Time Frame

The time frame for completion of this research work is mentioned below:

Table No. 3.1

Time Frame (Ph.D THESIS)	
July 2013-December 2013	Literature Survey, Concept Development and Design
January 2014-June 2014	Implementation and Testing
July 2014-December 2014	Evaluation and Redesign (if any)
	Thesis Writing and Paper presentation
January 2015-June 2015	Thesis Writing

References

[1] A.W. Min, K.G. Shin, "Robust tracking of small scale primary user in cognitive radio networks," IEEE transactions on Parallel and distributed systems, Vol. 24, no.4, pp. 778-787, April, 2013.

[2] A. D. Domenico, E.C. Strinati, M.D Benedetto, "A Survey on MAC Strategies for cognitive radio networks," IEEE Communications surveys & tutorials, Vol. 14, no. 1, 2012.

[3] A. Attar, H.Tang, A.V Vasilakos, F. Richard, V.C.M Leung, "A survey of Security Challenges in cognitive radio networks: Solutions and future research directions," Proceedings of the IEEE, Vol. 100, no. 12, pp. 3172-3183, Dec. 2012.

[4] Van Tam Nguyen, Frederic Villain, and Yann Le Guillou,"Cognitive Radio RF Overview and Challenges", 2012 ,Article ID 716476.

[5] A. Garhwal, P.P Bhattacharya, "A Survey on spectrum sensing techniques in cognitive radio," International Journal of Computer science & Communication Networks, Vol. 1, pp. 196-206, 2011.

[6] NishaYadav, SumanRathi, "Spectrum Sensing Techniques: Research, Challenge and Limitations", IJECT, ISSN : 2230-7109, Dec. 2011.

[7] O. Leon, J.Hernandez-Serrano and M.Soriano, "Securing Cognitive Radio Networks," International Journal of communication systems, Vol. 23, pp. 633-652, Feb. 2010.

[8] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," IEEE Communications Surveys &Tutorials, Vol. 11, no. 1, pp. 116–130, 2009.

[9] A. W. Min, K. G. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," Proc. Of 17th IEEE Int. Conf. Network Protocols, Princeton, NJ, pp. 294–303, Oct. 13–16, 2009.

[10] T. Qin, H. Yu, C. Leung, Z. Shen, and C.Miao, "Towards a trust aware cognitive radio architecture," ACM Mobile Comput. Commun. Rev., Vol. 13, no. 2, pp. 86–95, Apr. 2009.

[11] W. Wangz, H. Liy, Y. Sunz, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," Proc. Conf. Inf. Sci. Syst., Baltimore, MD, Mar. 2009.

[12] P. Kaligineedi, M. Khabbazian and Vijay K. Bhargava, "Secure Cooperative Sensing techniques for Cognitive Radio Systems," pp. 3406-3410, ICC 2008.

[13] T.C Clancy, N. Georgen, "Security in Cognitive radio networks: Threats and Mitigation," CrownCom 2008, pp.1-8, 15-17 May, 2008.

[14] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," Mobile Net. Appl., vol. 13, no. 5, pp. 516–532, Oct. 2008.

[15] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," Proc. IEEE Int. Conf. Commun., Beijing, China, pp. 3406–3410, May 2008.

[16] I.F Akyildiz, W Lee, M.C Vuran, S Mohanty, "Next Generation/ Dynamic spectrum access/cognitive radio wireless networks: A survey," Computer Networks 50 2127-2159, May 2006.

[17] I.F. Akyildiz, X. Wang, W. Wang, "Wireless mesh networks: a survey," Computer Networks Journal, pp. 445–487, 2005.

[18] A. Ghasemi and E. S. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environment", in Proc. IEEE DySPAN, pp. 131-136, Nov. 2005.

[19] J.A. Stine, "Spectrum management: the killer application of ad hoc and mesh networking," Proc. IEEE DySPAN 2005, pp. 184–193, Nov. 2005.

[20] D. Maldonado, B. Lie, A. Hugine, T.W. Rondeau, C.W. Bostian, "Cognitive radio applications to dynamic spectrum allocation," Proc. IEEE DySPAN 2005, pp. 597–600 November 2005.

[21] R. Murty, Software-defined Reconfigurability radios: smart, agile, cognitive, and interoperable, Technology@Intel Magazine, July 2003.

[22] M. Oner and F. Jondral, "Cyclostationarity based air interface recognition for software radio systems," in Proc. IEEE Radio and Wireless Conf., Atlanta, Georgia, USA, , pp. 263–266, Sept. 2004.

[23] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," Personal Communications, IEEE, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[24] Jospeh Mitola III. Software radios-survey, critical evaluation and future directions. In IEEE National Telesystems Conference, pages 13/15–13/23, 1992.

[25] http://www.radio-electronics.com/info/rf-technology-design/cognitive-radio-cr/technology-tutorial.php

[26] http://www.fcc.gov/oet/info/database/spectrum/

[27] http://www.ece.gatech.edu/research/labs/bwn/CR/projectdescription.html

[28] http://www.trai.gov.in